Thanatos Ransomware Is First to Use Bitcoin Cash. Messes Up Encryption

bleepingcomputer.com/news/security/thanatos-ransomware-is-first-to-use-bitcoin-cash-messes-up-encryption

By
Lawrence Abrams

- February 26, 2018
- 12:56 PM
- 0

Ransomware developers continue to release infections that are clearly not tested well and contain bugs that may make it difficult, if not impossible, for victims to recover their files. Such is the case with the new in the wild ransomware called Thanatos that has been discovered by security researcher MalwareHunterTeam.

When the Thanatos Ransomware infects a victim it will use a new key for each encrypted file. The problem, according to researcher Francesco Muroni, is that these keys are never saved anywhere. This means that if a user pays the ransom, the ransomware developer does not have a method that will actually be able to decrypt each file. Therefore, it is not recommended that victims pay the Thanatos ransom for any reason.

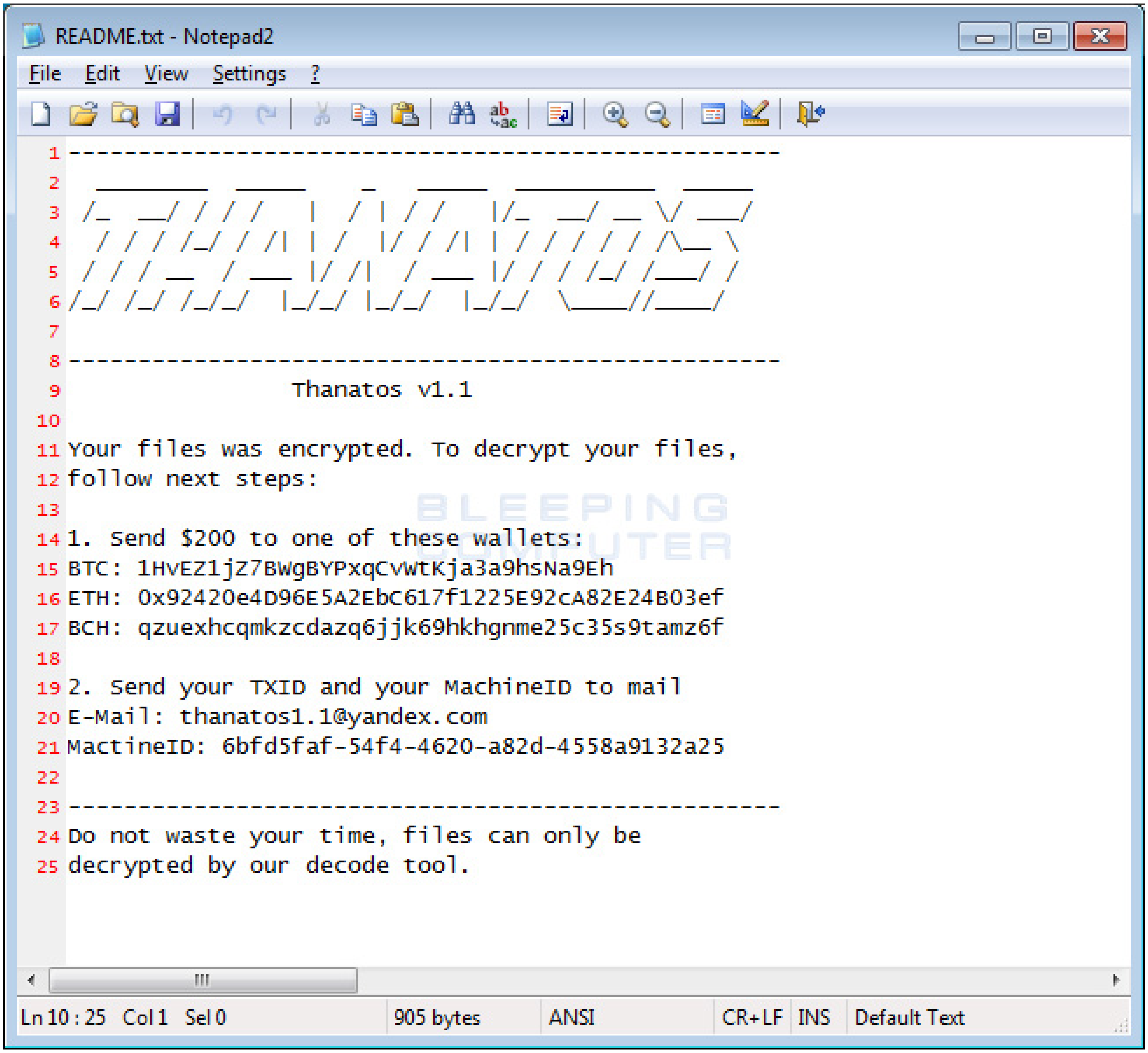
The good news is that according to Muroni it may be possible to brute force the encryption key for each file. This would take quite a bit of time and would require the file to be a common file type with a known magic header.

Thanatos is the first ransomware to accept Bitcoin Cash

While the encryption part of Thanatos is a mess, the ransomware does introduce something new. That is being the first ransomware to accept Bitcoin Cash as a ransom payment.

For those unfamiliar with Bitcoin Cash, it is a new cryptocurrency that was spun off from Bitcoin. When Bitcoin hit block 478,558, Bitcoin was forked into a new cryptocurrency called Bitcoin Cash. When this fork occurred, Bitcoin holders were then given an equivalent amount of Bitcoin Cash. For example, if a user had 2 Bitcoins at the time of the fork, they would have received 2 Bitcoin Cash as well.

While Thanatos accepts both Bitcoin and Etherum as a ransom payment, this is the first time that Bitcoin Cash has been accepted as shown in the ransom note below.



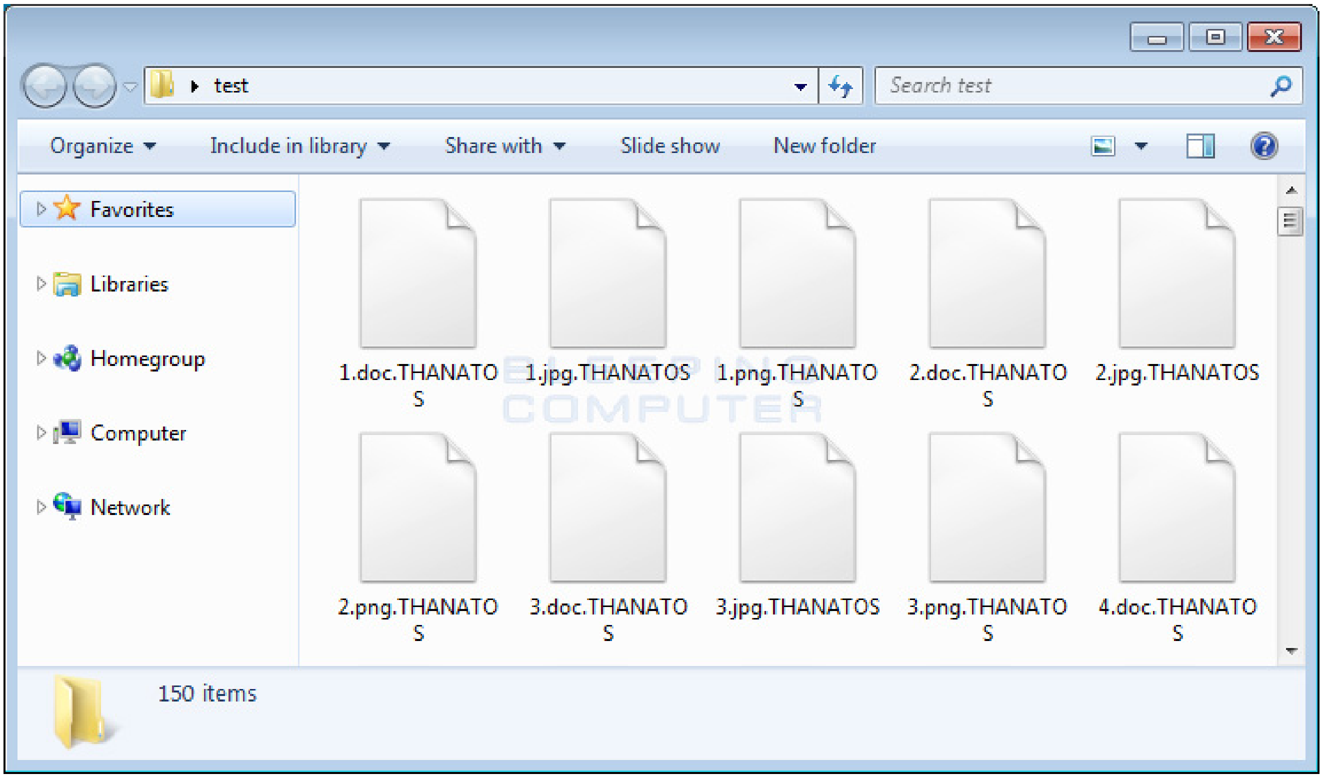
```
----------------------------------------------------
  ________  _____    _   _____  __________  _____
 /_  __/ / / /   |  / | / /   |/_  __/ __ \/ ___/
  / / / /_/ / /| | /  |/ / /| | / / / / / /\__ \
 / / / __  / ___ |/ /|  / ___ |/ / / /_/ /___/ /
/_/ /_/ /_/_/  |_/_/ |_/_/  |_/_/  \____//____/

----------------------------------------------------
                Thanatos v1.1

Your files was encrypted. To decrypt your files,
follow next steps:

1. Send $200 to one of these wallets:
BTC: 1HvEZ1jZ7BWgBYPxqCvWtKja3a9hsNa9Eh
ETH: 0x92420e4D96E5A2EbC617f1225E92cA82E24B03ef
BCH: qzuexhcqmkzcdazq6jjk69hkhgnme25c35s9tamz6f

2. Send your TXID and your MachineID to mail
E-Mail: thanatos1.1@yandex.com
MactineID: 6bfd5faf-54f4-4620-a82d-4558a9132a25

----------------------------------------------------
Do not waste your time, files can only be
decrypted by our decode tool.
```

Thanatos Ransom Note

How Thanatos Ransomware encrypts a Computer

When the Thanatos Ransomware encrypts a computer it will generate a new encryption key for every file encrypted. As discussed already, unfortunately these encryption keys are not saved anywhere and thus according to researchers it would not be possible for the developers to decrypt the files even if a ransom payment is made.

When encrypting files it will append the .THANATOS extension to an encrypted file's name. For example, a file named test.jpg would be encrypted and renamed as test.jpg.THANATOS.



Thanatos Encrypted Files

After the encryption process is finished it will then connect to iplogger.com/1t3i37 URL in order to keep track of the amount of victims that have been infected.

Finally, it will generate an autorun key called "Microsoft Update System Web-Helper" that opens the README.txt ransom note every time a user logs in. This ransom note can be seen in the article's previous section.

This ransom note contains instructions to send a $200 USD ransom payment to one of the listed Bitcoin, Ethereum, or Bitcoin Cash addresses. The user is then instructed to contact thanatos1.1@yandex.com with their unique victim ID in order to receive a decryption program.

As already stated, this ransomware can not be decrypted normally due to it not saving the encryption keys and thus the ransom payment should not be made. If anyone is infected with this ransomware, they should contact us about the possible creation of a brute force program.

How to protect yourself from the Thanatos Ransomware

In order to protect yourself from ransomware in general, it is important that you use good computing habits and security software. First and foremost, you should always have a reliable and tested backup of your data that can be restored in the case of an emergency, such as a ransomware attack.

You should also have security software that incorporates behavioral detections to combat ransomware and not just signature detections or heuristics. For example, Emsisoft Anti-Malware and Malwarebytes Anti-Malware both contain behavioral detection that can prevent many, if not most, ransomware infections from encrypting a computer.

Last, but not least, make sure you practice the following security habits, which in many cases are the most important steps of all:

- Backup, Backup, Backup!
- Do not open attachments if you do not know who sent them.
- Do not open attachments until you confirm that the person actually sent you them,
- Scan attachments with tools like VirusTotal.
- Make sure all Windows updates are installed as soon as they come out! Also make sure you update all programs, especially Java, Flash, and Adobe Reader. Older programs contain security vulnerabilities that are commonly exploited by malware distributors. Therefore it is important to keep them updated.
- Make sure you use have some sort of security software installed that uses behavioral detections or white list technology. White listing can be a pain to train, but if your willing to stock with it, could have the biggest payoffs.
- Use hard passwords and never reuse the same password at multiple sites.

For a complete guide on ransomware protection, you visit our How to Protect and Harden a Computer against Ransomware article.

Related Articles:

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

US Senate: Govt’s ransomware fight hindered by limited reporting

New RansomHouse group sets up extortion market, adds first victims

Ransomware attack exposes data of 500,000 Chicago students

IOCs

Hashes:

```
fe1eafb8e31a84c14ad5638d5fd15ab18505efe4f1becaa36eb0c1d75cd1d5a9
```

Ransom Note Text:

```
---------------------------------------------------
  ________  _____    _   _____  __________  _____
 /_  __/ / / /   |  / | / /   |/_  __/ __ \/ ___/
  / / / /_/ / /| | /  |/ / /| | / / / / / /\__ \
 / / / __  / ___ |/ /|  / ___ |/ / / /_/ /___/ /
/_/ /_/ /_/_/  |_/_/ |_/_/  |_/_/  \____//____/

---------------------------------------------------
                Thanatos v1.1

Your files was encrypted. To decrypt your files,
follow next steps:

1. Send $200 to one of these wallets:
BTC: 1HvEZ1jZ7BWgBYPxqCvWtKja3a9hsNa9Eh
ETH: 0x92420e4D96E5A2EbC617f1225E92cA82E24B03ef
BCH: qzuexhcqmkzcdazq6jjk69hkhgnme25c35s9tamz6f

2. Send your TXID and your MachineID to mail
E-Mail: thanatos1.1@yandex.com
MactineID: 6bfd5faf-54f4-4620-a82d-4558a9132a25

---------------------------------------------------
Do not waste your time, files can only be
decrypted by our decode tool.
```

Email Addresses:

```
thanatos1.1@yandex.com
```

Associated Files:

```
README.txt
```

Associated Registry Entries:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "Microsoft Update
System Web-Helper" = "C:\Windows\System32\notepad.exe
%UserProfile%\Desktop\README.txt"
```

- Ransomware
- Thanatos

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: